525 Rec'd PCT/PTO 27 NOV 2000

FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **1243-00**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **09/701200**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/26844	**29 SEP 00**	**01 OCT 99**

TITLE OF INVENTION
REGISTRY MONIORING SYSTEM AND METHOD

APPLICANT(S) FOR DO/EO/US
FRIEDMAN, George; STAREK, Robert Phillip; MURDOCK, Carlos

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ A copy of the International Search Report (PCT/ISA/210).
8. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☐ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

acknowledgement postcard

529 Rec'd PCT/PTC 27 NOV 2000

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR) 09/701200	INTERNATIONAL APPLICATION NO. PCT/US00/26844	ATTORNEY'S DOCKET NUMBER 1243-00

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1,000.00**
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO	**$860.00**
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$710.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$690.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =	**$710.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	20 - 20 =	0	x $18.00	**$0.00**	
Independent claims	5 - 3 =	2	x $80.00	**$160.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$870.00**	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.			☐	**$0.00**	
SUBTOTAL =				**$870.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	**$0.00**	
TOTAL NATIONAL FEE =				**$870.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☒	**$40.00**	
TOTAL FEES ENCLOSED =				**$910.00**	
				Amount to be: refunded	$
				charged	$

☒ A check in the amount of **$910.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **13-3405** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

PAUL A. TAUFER, ESQ.
SCHNADER HARRISON SEGAL & LEWIS, LLP
1600 MARKET STREET, SUITE 3600
PHILADELPHIA, PA 19103
(215) 751-2475
(215) 568-6946 (fax)

SIGNATURE

Paul A. Taufer
NAME

35,703
REGISTRATION NUMBER

November 27, 2000
DATE

REGISTRY MONITORING SYSTEM AND METHOD

FIELD OF THE INVENTION

The invention relates to the protection of data stored in a computer, and more particularly to data which has been imported from an outside source.

BACKGROUND OF THE INVENTION

A registry is a hierarchical repository for configuration data. The terms "information" and "data" as used herein are each intended to include the broadest definition of the other, and each include text, audio and video data. By way of further example, the term "information"can mean raw data, processed data, or a combination of raw and processed data. The registry may keep track of all software stored on the computer, and the relationship between programs. The registry may keep track of a plurality of users and hardware configurations. Preferences may vary among the plurality of users.

Each piece of data in the registry has a key-value associated with it. Together the name and value is referred to as a value entry. A key is analogous to a folder and may itself contain one or more folders, which may be referred to as subkeys, and one or more name-value pairs. The key may also be referred to as a name or a handle. To access the data and retrieve the stored value the correct key is needed.

Because the registry is a database, and thus, is a data storage location, it may be exploited for leaking data. "Leaking data" as used herein means transferring data out of a system in which it is desired to have the data secured. A process may write information to the registry, for example, for temporary storage. Another process may then access the information from the registry and write the data to a registry key. Another process may then read the data from the registry key and write it to a disk or other storage device, thereby leaking data. Accordingly, for applications wherein data security is important, there is a need to limit data leakage from the registry.

SUMMARY OF THE INVENTION

The invention discloses a registry monitoring method particularly applicable to a system

in which protected data is transmitted to a recipient computer. An illustrative embodiment of the invention comprises requesting a handle for a registry key to a calling process, requesting a registry key value for the handle, modifying and deleting keys and values of protected data locations, and obtaining security clearance to complete the requests by checking secured process lists and rejection lists.

Further disclosed are a registry monitoring system, a secured data transmission system including registry monitoring, a machine-readable medium comprising a program to monitor a registry, and a computer configured to monitor a registry.

DESCRIPTION OF THE DRAWINGS

The invention is best understood from the following detailed description when read with the accompanying figures.

FIGURE 1 is a diagram of a portion of a computer system according to an illustrative embodiment of the invention.

FIGURES 2 A-C are flow charts of a registry monitoring system according to an illustrative embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the invention disclosed comprise a method and system for monitoring a registry and may reduce or eliminate data leakage from the registry. The invention secures processes to deny data transfer to non-visual aspects of the system. This includes, for example, restricting writing to a file system, transferring data over communication ports, sharing memory with other processes and writing data to the registry.

An exemplary embodiment of the registry monitoring method comprises requesting a handle for a registry key to a calling process, requesting a registry key value for the handle, and obtaining security clearance to complete the requests by checking secured process lists and rejection lists. Because the ability to add to the registry is blocked, the ability to delete from the registry is also blocked. Therefore, the system includes a method for modifying and deleting keys and values with a security check incorporated therein.

The registry monitoring method of the present invention is best described as it may be carried out on a computer implemented secured data transmission system. An illustrative

example of such a system comprises two main components, a data packager and a receiver. The packager is used to create packages that carry file content to target recipients. The receiver runs on a recipient computer to allow access to packaged file content.

FIGURE 1 depicts an illustrative computer system 100 according to an embodiment of the invention. A registry entry guard driver 120 is in communication with file system hook driver 140. Both drivers exist on the kernel (ring 0) level 130. Applications 160 run on higher levels 140. When applications 160 request access to registry 110, guard driver 120 in conjunction with hook driver 140 monitors and handle the requests.

A package carries data and provides associated information to a command center which is a component of an application programming interface, such as a Win32 process. A communication driver handles communication between the application programming interface and a plurality of device drivers. It provides a single set of device driver I/O control functions that are called from the application programming interface to send information to or retrieve information from the device drivers. The communication driver is called by a hook driver to notify the command center that a process is trying to open a packaged file. The device drivers, together with the application programming interface, marshal the packaged content into a vault and support access to the content, subject to an originator's permission selection. The command center may watch for packages to be executed and prompt users for file names to save a package payload. It may notify the file system hook driver that a package payload should be absorbed into the vault. It may present users with dialog indicating that an application is attempting to open a packaged file. It may also notify device drivers 106 when applications exit. The command center may block clipboard access and terminate applications at the request of a permissions device driver when permissions expire. Permission information is contained in a database and may include, for example, file names, package ID, file system ID and file permissions. File permissions may include, but are not limited to, length of time or number of times a file may be open, date after which a file may no longer be opened, and printing and clipboard permissions.

File system hook driver 140 obtains a data request initiated from a user who is looking to access a packaged or absorbed file. When hook driver 140 receives the requests it performs a security check on the process and then queries the user. The process is then added to a secured process list. The registry monitor is notified that the process is secured so it may block access in the future.

FIGURES 2 A-C depict an illustrative embodiment of the invention. Those skilled in the

art will understand that variations on the registry monitoring system that include security checks to block access to keys and values are equivalent to the steps described herein, and thus, are within the spirit and scope of the invention. FIGURE 2A depicts an illustrative filtering sequence for a registry open key call. The call is made to obtain a handle for a registry key to a calling process. The registry key handle call is made in step 302. In step 304 a process ID and registry key are determined. Based on this information it is determined in step 306 whether the process is secured by checking a secured process list. The secured process list is continually updated as processes successfully request secured data from the hook driver and process quit calls are initiated. If the process is secured, then in step 308 it is determined whether the registry key is on a rejection list. If the registry key is on the rejection list, the process is denied access to the registry key in step 310 and the call is successfully filtered in step 312. If the process is not on the secured list or if the registry key name is not on the rejection list, then in step 314 the request is completed and the call is successfully filtered in step 312.

FIGURE 2B is an illustrative flow chart for a registry key value call filtering sequence. A registry key value for the handle is requested in step 316. The process ID and registry key name are determined in step 318. In step 320 the secured process list is again consulted to determine whether the process is secured. If the process is secured, it is determined in step 322 whether the registry key is on a rejection list. If the registry key is on the rejection list, the process is denied access to the registry key value in step 324, and the call is successfully filtered in block 326. If the process is not on the secured list, the request is completed in step 328, and the call is successfully filtered in block 326. If the registry key is not on the rejection list and the process is on the secured process list, the value request is processed in step 330 and it is determined whether the value is on the rejection list in step 332. If the value is not on the rejection list the request is allowed to be completed in step 328, and the call is successfully filtered in block 326. If the value is on the rejection list then in step 324 access is denied to the registry key value, and the call is successfully filtered in block 326.

Handles and values may then be deleted or modified. An exemplary flow chart for a deletion or modification sequence is depicted in FIGURE 3C. A delete or set-value call is made in step 334. The process ID is then determined in step 336. In step 338 it is then determined whether the process is secured by checking whether the process is on the secured process list. If the process is not on the secured process list, the request is completed in step 340 and the call is successfully filtered in step 342. If the process is on the secured process list, the request is not allowed to be completed in step 344 and the call is successfully filtered in step 342.

Further disclosed is a registry monitoring system wherein the registry is monitored according to methods described herein. Additionally, an embodiment of the invention includes a computer configured to monitor a registry according such methods. The terms "computer" or "computer system" as used herein include any device capable of receiving, transmitting, and/or using information, including, without limitation, a processor, a microprocessor, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television or electronic box attached to a television, such as for example, a television adapted to be connected to the Internet, a cellular telephone, a personal digital assistant, an electronic pager, and a digital watch In an illustrative example information is transmitted in the form of e-mail. Embodiments of the invention still further include a machine-readable medium comprising a program to monitor a registry according to methods described herein.

While the invention has been described by illustrative embodiments, additional advantages and modifications will occur to those skilled in the art. Therefore, the invention in its broader aspects is not limited to specific details shown and described herein. Modifications, for example, to steps for obtaining security clearance to complete requests, may be made without departing from the spirit and scope of the invention. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments but be interpreted within the full spirit and scope of the appended claims and their equivalents.

What is claimed is:

1. A method of monitoring a registry comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests.

2. The method of claim 1 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

3. The method of claim 1 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

4. The method of claim 1 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

5. A registry monitoring system wherein the registry is monitored by a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests.

6. The registry monitoring system of claim 5 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

7. The registry monitoring system of claim 5 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

8. The registry monitoring system of claim 5 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

9. A computer configured to monitor a registry according to a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests.

10. The computer of claim 9 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

11. The computer of claim 9 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

12. The computer of claim 9 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

13. A machine-readable medium comprising a program to monitor a registry according to a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests.

14. The machine-readable medium of claim 13 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

15. The machine-readable medium of claim 13 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

16. The machine-readable medium of claim 13 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

17. A computer implemented secured data transmission system having a receiver to access secured file content provided by a sender, wherein the receiver includes a registry monitoring

system wherein the registry is monitored by a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests.

18. The computer implemented secured data transmission system of claim 17 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

19. The computer implemented secured data transmission system of claim 17 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

20. The computer implemented secured data transmission system of claim 17 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

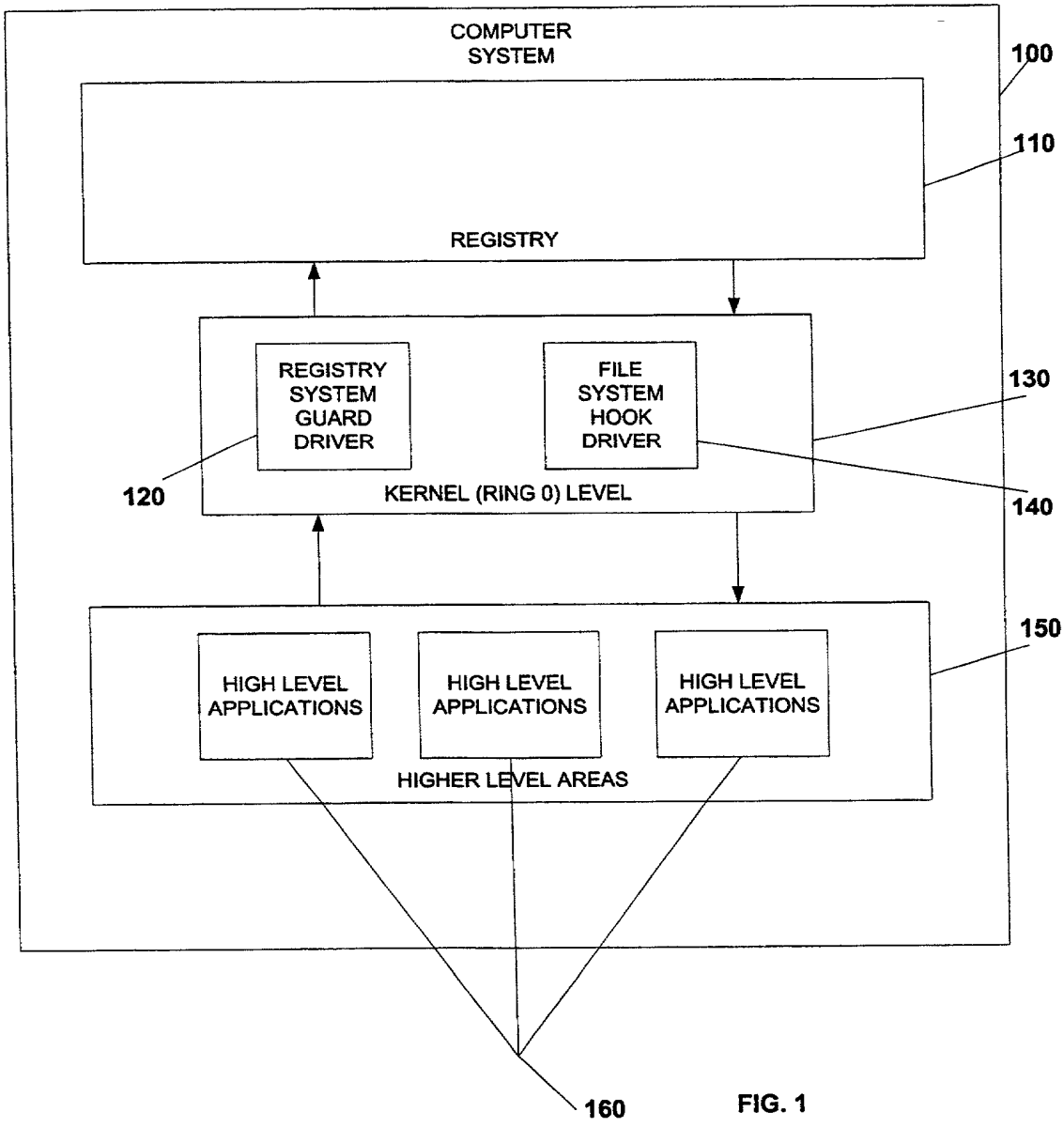
COMPUTER SYSTEM
100
110
REGISTRY
REGISTRY SYSTEM GUARD DRIVER
FILE SYSTEM HOOK DRIVER
130
120
KERNEL (RING 0) LEVEL
140
150
HIGH LEVEL APPLICATIONS
HIGH LEVEL APPLICATIONS
HIGH LEVEL APPLICATIONS
HIGHER LEVEL AREAS
160

FIG. 1

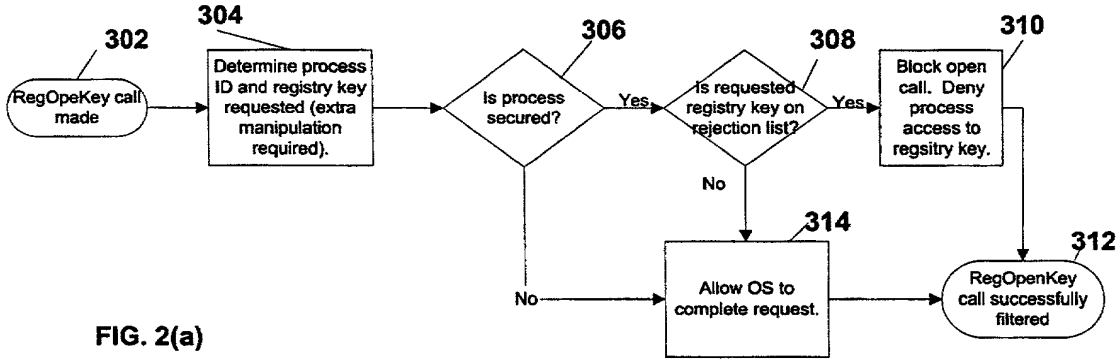

FIG. 2(a)

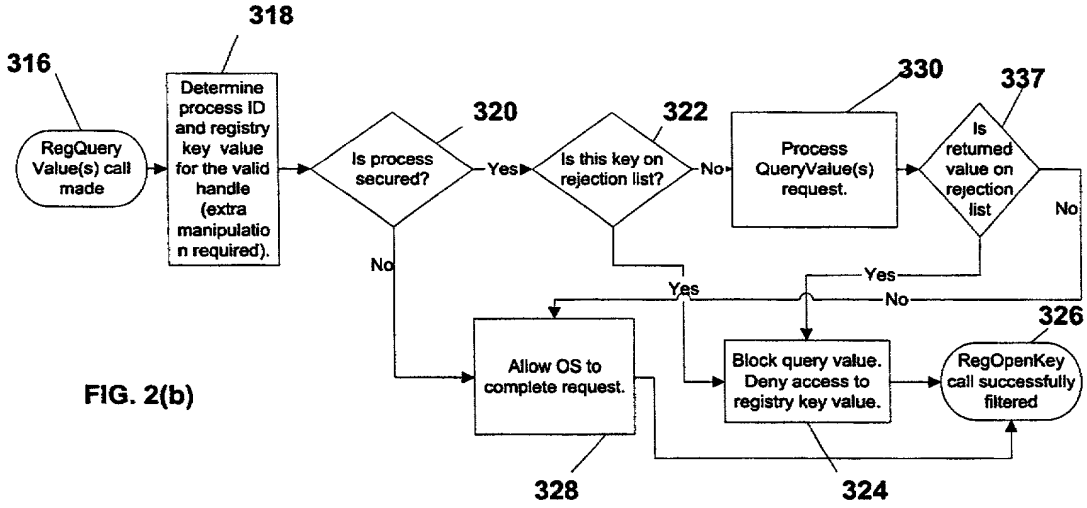

FIG. 2(b)

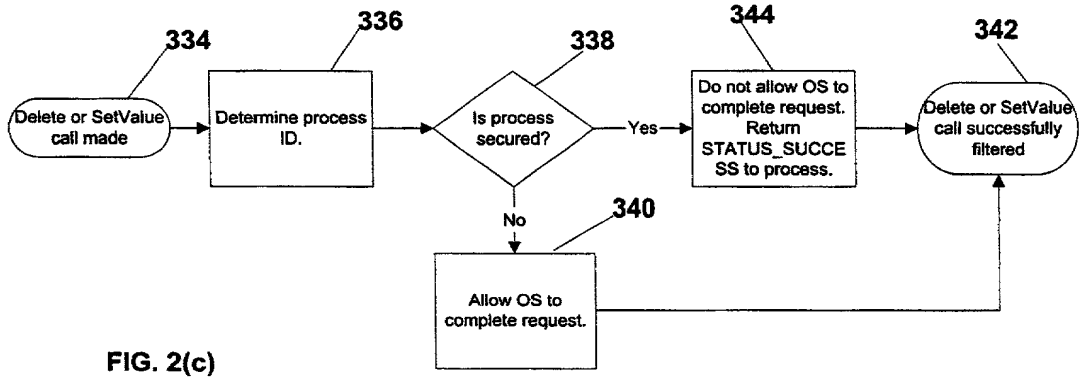

FIG. 2(c)

Doc. No. 1243-00

Declaration and Power of Attorney for Patent Application

As the below named inventor, we hereby declare that:

Our residence, post office address and citizenship are as stated next to our names,

We believe we are the original and first inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled REGISTRY MONITORING SYSTEM AND METHOD the specification of which is filed herewith.

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the application:

PCT/US00/26844	9/29/00	pending
(Application Serial No.)	(Filing Date)	(Status) (patent, pending, abandoned)

We hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

T. Daniel Christenbury	Reg. No. 31,750
Guy T. Donatiello	Reg. No. ~~33,167~~
Paul A. Taufer	Reg. No. 35,703
Austin R. Miller	Reg. No. ~~16,602~~
James A. Drobile	Reg. No. ~~19,690~~
Gerard J. Weiser	Reg. No. 19,763
Robert A. McKinley	Reg. No. 43,793
Michael A. Patané	Reg. No. 42,982
Joan T. Kluger	Reg. No. 38,940
Sharon Fenick	Reg. No. ~~45,269~~
Stewart M. Wiener	Reg. No. 46,201
Armando A. Flores	Reg. No. 41,754
Felicity Rowe	Reg. No. 47,042

13

Address all telephone calls to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103 (215) 751-2475.

Address all correspondence to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103.

We hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

1-02

Full name of first and joint inventor: George Friedman

Inventor signature _____ TX

11/15/2000
Date

Residence: 7109 Montana Norte, Austin, Texas 78727
Citizenship: USA
Mailing Address: same as above

2-02

Full name of second and joint inventor: Robert Phillip Starek

Inventor signature Robert P. Starek

11/15/2000
Date

Residence: 1807 W. Slaughter Lane #200-482, Austin, Texas 78748 TX
Citizenship: USA
Mailing Address: same as above

3-00

Full name of third and joint inventor: Carlos A. Murdock

Inventor signature ______________ 11/15/2000
Date

Residence: 4517 Avenue F, Austin, Texas 78751 TX
Citizenship: USA
Mailing Address: same as above